



(12) **EUROPEAN PATENT APPLICATION**
 published in accordance with Art. 153(4) EPC

(43) Date of publication:
03.02.2016 Bulletin 2016/05

(51) Int Cl.:
H04L 12/46^(2006.01) H04L 12/70^(2013.01)
H04L 12/749^(2013.01)

(21) Application number: **14775639.9**

(86) International application number:
PCT/JP2014/001338

(22) Date of filing: **10.03.2014**

(87) International publication number:
WO 2014/156009 (02.10.2014 Gazette 2014/40)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
 Designated Extension States:
BA ME

(72) Inventor: **MIYAMOTO, Takahiro**
Fujimino-shi
Saitama 356-8502 (JP)

(30) Priority: **26.03.2013 JP 2013064872**

(74) Representative: **Pitchford, James Edward et al**
Mathys & Squire LLP
The Shard
32 London Bridge Street
London SE1 9SG (GB)

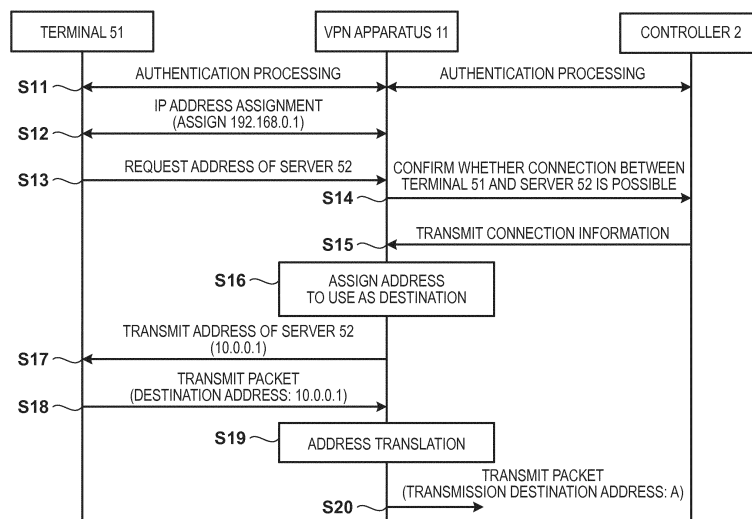
(71) Applicant: **KDDI Corporation**
Tokyo 163-8003 (JP)

(54) **TRANSFER DEVICE**

(57) A transfer apparatus that connects a first network and a virtual private network and performs transferring of a packet between the first network and the virtual private network, comprising: a determination unit for determining, when a request to communicate with a second communication apparatus of the second network or a query for an address of the second communication apparatus is received from a first communication apparatus of the first network, whether communication between the first communication apparatus and the second communication

apparatus via the virtual private network is permitted; and an address determination unit for, when communication between the first communication apparatus and the second communication apparatus via the virtual private network is permitted, determining a destination address that the first communication apparatus uses when communicating with the second communication apparatus, and notifying the first communication apparatus of the destination address.

FIG. 3



Description

TECHNICAL FIELD

[0001] The present invention relates to a technique for name resolution in a virtual private network (VPN).

BACKGROUND ART

[0002] VPNs are used for interconnection of local area networks (LANs) in a plurality of locations of a company. Communication apparatuses in a LAN, other than communication apparatuses that are open to the Internet, use only private IP (Internet Protocol) addresses. Accordingly, cases may exist in which two communication apparatuses that are connected to different LANs are using the same IP address. For this reason, Patent Document 1 discloses a configuration in which an address translation is performed when IP addresses in different LANs are the same. Also, Patent Document 2 discloses a VPN management apparatus that collectively controls VPN apparatuses that connects a plurality of LANs via VPN.

CITATION LIST

PATENT LITERATURE

[0003]

[Patent Document 1] Japanese Patent Laid-Open No. 2005-142702

[Patent Document 2] Japanese Patent Laid-Open No. 2003-101569

SUMMARY OF INVENTION

TECHNICAL PROBLEM

[0004] Currently, use of VPNs in order to interconnect LANs of different companies has started. When LANs of different companies are connected by VPNs, for reasons of security, it is necessary to restrict communication via the VPN such that it is only possible between specific communication apparatuses, rather than permitting communication between any of the communication apparatuses connected to the LANs of the different companies. Also, because the communication apparatuses within the LANs are usually using private IP addresses, name resolution for a communication apparatus that is connected only to a LAN of a company cannot be performed in a DNS (Domain Name System) that can be used on the Internet. Furthermore, there are cases in which two communication apparatuses that are connected to LANs of different companies are using the same IP addresses.

[0005] Patent Document 1 discloses a configuration in which overlapping IP addresses are translated, but cannot control so as to permit communication by only specific communication apparatuses. Also, by the methods dis-

closed in Patent Documents 1 and 2, name resolution of a destination communication apparatus that is connected to a LAN of another company cannot be performed.

5 SOLUTION TO PROBLEM

[0006] According to one embodiment of the present invention, a transfer apparatus that, for communication between a communication apparatus of a first network and a communication apparatus of a second network via a virtual private network, connects the first network and the virtual private network and performs transferring of a packet between the first network and the virtual private network, the transfer apparatus comprising: determination means for determining, when a request to communicate with a second communication apparatus of the second network or a query for an address of the second network is received from a first communication apparatus of the first network, whether communication between the first communication apparatus and the second communication apparatus via the virtual private network is permitted; and address determination means for, when communication between the first communication apparatus and the second communication apparatus via the virtual private network is permitted, determining a destination address that the first communication apparatus uses when communicating with the second communication apparatus, and notifying the first communication apparatus of the destination address.

[0007] Other features and advantages of the present invention will be apparent from the following description taken in conjunction with the accompanying drawings. Note that the same reference numerals denote the same or like components throughout the accompanying drawings.

BRIEF DESCRIPTION OF DRAWINGS

[0008] The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate embodiments of the invention and, together with the description, serve to explain the principles of the invention.

45 FIG. 1 is a system configuration diagram according to an embodiment.

FIG. 2 is a configuration diagram for a VPN apparatus according to an embodiment.

50 FIG. 3 is a sequence diagram for name resolution and address assignment according to an embodiment.

FIG. 4 is a sequence diagram for name resolution and address assignment according to an embodiment.

55 FIG. 5A is a view for illustrating information that a controller holds according to an embodiment.

FIG. 5B is a view for illustrating information that the controller holds according to an embodiment.

FIG. 5C is a view for illustrating information that a VPN apparatus holds according to an embodiment.

DESCRIPTION OF EMBODIMENTS

[0009] Exemplary embodiments of the present invention will be described hereinafter with reference to the drawings. Note that elements that are not necessary for the explanation of the embodiments are omitted from the figures below.

[0010] FIG. 1 is a system configuration diagram used for explanation of an embodiment. In FIG. 1, a VPN apparatus 11 is connected to VPN apparatuses 12 and 13 via a VPN 4. Note that in the present embodiment, VPN apparatus means a transfer apparatus that performs a relay between a VPN (Virtual Private Network) and a LAN (Local Area Network). Also, in the example of FIG. 1, LANs 31, 32 and 33 are respectively company networks of different companies. Note that in FIG. 1, a terminal 51, a server 52, and a server 53, which are communication apparatuses, are respectively connected to the LAN 31, the LAN 32 and the LAN 33. A controller 2, for example, is installed by a communications carrier that provides the VPN 4, and the controller 2 holds connection information indicating which communication apparatuses of which companies communication is permitted between, and addresses used in the VPN 4 for permitted communication between apparatuses. Note that though not shown, the LANs 31, 32 and 33 are connected to the Internet. Below, explanation of an embodiment will be given assuming using the configuration of FIG. 1 as an example.

[0011] An example of connection information that the controller 2 holds is illustrated in FIG. 5A. An entry having a number #1 in FIG. 5A indicates that communication by the terminal 51 of the LAN 31 and the server 52 of the LAN 32 via the VPN 4 is permitted. Furthermore the entry having the number #1 indicates that when the terminal 51 of the LAN 31 and the server 52 of the LAN 32 communicate via the VPN 4, in the VPN 4, address X is used as an address of the terminal 51, and address A is used as an address of the server 52. Additionally, it is assumed that a combination of the terminal 51 of the LAN 31 and the server 53 of the LAN 33 is something that is not included in the connection information of FIG. 5A. Accordingly, the connection information of FIG. 5A indicates that communication by the terminal 51 of the LAN 31 and the server 53 of the LAN 33 via the VPN 4 is not permitted.

[0012] FIG. 3 illustrates a sequence for when the terminal 51 of the LAN 31 and the server 52 of the LAN 32 communicate. In step S11, the terminal 51 performs authentication processing with the VPN apparatus 11. Note that for the authentication processing, for example, a method that complies with IEEE 802.1X can be used. In the present embodiment, it is assumed that the VPN apparatus 11 transmits to the controller 2 authentication information that the terminal 51 transmits in the authentication processing, and the controller 2 performs an authentication of the terminal 51, and transmits an authentication

result to the VPN apparatus 11. However, authentication may be performed on the VPN apparatus 11. Also, when the authentication of the terminal 51 succeeds, the VPN apparatus 11 saves for a predetermined period something to that effect. By this configuration, it is possible to omit processing between the VPN apparatus 11 and the controller 2 in step S11 when the VPN apparatus 11 holds information that the authentication of the terminal 51 already succeeded.

[0013] In step S12, the VPN apparatus 11 assigns an IP address of the terminal 51. Note that when an IP address is already assigned to the terminal 51, the processing of step S12 is omitted. In step S13, the terminal 51 transmits a request to communicate with the server 52 to the VPN apparatus 11 in order to communicate with the server 52. The request to communicate is a message for querying an IP address of the server 52 which includes identification information of the server 52. Note that for the identification information of the server 52, for example, a fully qualified domain name can be used. The VPN apparatus 11, in step S14, queries the controller 2 as to whether communication via the VPN 4 between the terminal 51 and the server 52 is permitted. In the present example, as is illustrated in FIG. 5A, because communication via the VPN 4 between the terminal 51 and the server 52 is permitted, the controller 2 transmits connection information corresponding to the entry having the number #1 in FIG. 5A to the VPN apparatus 11 in step S15.

[0014] The VPN apparatus 11, when it receives the connection information from the controller 2, generates, in step S16, an address that the terminal 51 uses as a destination address in the communication between the terminal 51 and the server 52. Here, it is assumed that 10.0.0.1 is generated. The VPN apparatus 11, in step S17, notifies the terminal 51 of the address generated in step S16. Also, the VPN apparatus 11 manages the address, which notifies as the address of the server 52 in association with the address assigned to the terminal 51, as is illustrated in FIG. 5C.

[0015] When, in step S18, the terminal 51 transmits a packet that has the address of the server 52 as a destination address, the VPN apparatus 11, translates, in step S19, the transmission source address, i.e. 192.168.0.1 and the destination address, i.e. 10.0.0.1 to the address X and the address A respectively, in accordance with the information illustrated in FIG. 5C, and transmits to the VPN apparatus 12 in step S20.

[0016] Note that the VPN apparatus 12 makes a query to the controller 2 when a communication apparatus on the LAN 32 corresponding to the destination address A cannot be identified. Also, because the VPN apparatus 11 saves the information illustrated in FIG. 5C in step S16, thereafter the packet is transferred in accordance with the information illustrated in FIG. 5C when a packet having 10.0.0.1 as a destination address is received from the terminal 51, and the processing from step S11 to step S17 becomes unnecessary. Additionally, configuration

may be taken in which, for example, a validity period is provided for the information illustrated in FIG. 5C, where the information is discarded after the validity period has elapsed. With this, even when a setting of the controller 2 is changed, the change can be reflected in the VPN apparatus 11.

[0017] A VPN apparatus according to this embodiment queries the controller 2 which manages the VPN 4 as to whether communication between communication apparatuses on different LANs is permitted, and if it is permitted, the VPN apparatus itself determines an address to be used as a destination, and communicates that to the communication apparatus which is the source of the request for communication. The address that is determined here can be determined to be an address that does not overlap with an address of a communication apparatus on the LAN to which the VPN apparatus is connected irrespective of the address that the actual communication partner is using. For example, the determined address can be made to be an address of a subnet that is different to that of the LAN to which the VPN apparatus is connected. Additionally, the determined address can be made to not overlap with an address already communicated as a destination address to each of the communication apparatuses in the LAN to which the VPN apparatus is connected. However, if a communication apparatus that a destination address indicates is specified by a set of a transmission source address and the destination address, the determined address may be made to be different to what was already communicated as a destination address to the communication apparatus which is the source of the request for the communication. In such a case, when the VPN apparatus receives a packet, the destination communication apparatus is identified based on the set of the transmission source address and the destination address, and translation into the address used by the VPN 4 is performed. By this configuration, the degree of freedom in determination of the destination address on the VPN apparatus is increased. By the above configuration, it is possible to solve a problem of IP address overlapping in a connection via the VPN 4 between different LANs, and provide name resolution. Also, it is possible to limit communication via the VPN 4 to between permitted communication apparatuses.

[0018] FIG. 4 illustrates a sequence for when the terminal 51 of the LAN 31 and the server 53 of the LAN 33 communicate. Note that communication via the VPN 4 is not permitted between the terminal 51 and the server 53 as was explained previously. Additionally, in the present example, the server 53 is a server that is available on the Internet, and accordingly, communication via the Internet between the terminal 51 and the server 53 is possible.

[0019] Step S31 and step S32 of FIG. 4 are the same as step S11 and step S12 of FIG. 3, and so explanation of these once again will be omitted. In step S33, the terminal 51 queries the IP address of the server 53 by transmitting identification information of the server 53 to the

VPN apparatus 11 in order to communicate with the server 53. The VPN apparatus 11, in step S34, queries the controller 2 as to whether communication via the VPN 4 between the terminal 51 and the server 53 is permitted. In the present example, because communication via the VPN 4 is not permitted between the terminal 51 and the server 53, the controller 2, in step S35, notifies the VPN apparatus 11 that it is not permitted.

[0020] Because, in this case, the communication between the terminal 51 and the server 53 is via the Internet, the VPN apparatus 11, in step S36, queries an external DNS server for the IP address of the server 53, thereby obtaining an IP address for accessing the server 53 via the Internet. After that, the VPN apparatus 11, in step S37, communicates the IP address of the server 53 obtained in step S36 to the terminal 51. In step S38, the terminal 51 accesses the server 53 via the Internet using the IP address communicated from the VPN apparatus 11. Note that in the present example, in a case where the server 53 is a communication apparatus that is not open to the Internet, the VPN apparatus 11 cannot obtain the IP address of the server 53 in step S36, and accordingly communicates something to that effect to the terminal 51 in step S37.

[0021] Additionally, in the explained embodiment, the controller 2 holds information indicating a set of two communication apparatuses capable of communicating via the VPN 4. However, if, for example, communication is possible between any two of a plurality of communication apparatuses, the controller 2 can manage the plurality of the communication apparatuses capable of communicating with each other as a group, as is illustrated in FIG. 5B. For example, in FIG. 5B it is illustrated that two groups, #1 and #2, exist, and the terminal 51 belongs to both groups. Here, all communication is permitted via the VPN 4 for any two of the communication apparatuses in group #1, even if they belong to different LANs, for example. Accordingly, when, in step S14 of FIG. 3, for example, a query as to whether or not communication is permitted between the terminal 51 and the server 52 is received, the controller 2 can transmit to the VPN apparatus 11 the group information of group #1 illustrated in FIG. 5B as the connection information. Alternatively, an embodiment may transmit VPN side addresses for the terminal 51 and the server 52 in the group information, and a group identifier. The VPN apparatus 11 manages the received group identifier by adding it to the information illustrated in FIG. 5C. For example, without querying the controller 2, the VPN apparatus 11 can determine, by receiving the same group identifier from the controller 2 in name resolution in communication with another communication apparatus, that this other communication apparatus and the terminal 51 or the server 52 can communicate via the VPN 4.

[0022] FIG. 2 is an overview configuration diagram for a VPN apparatus according to an embodiment. A transmission/reception unit 105 transmits/receives packets with a LAN, and a transmission/reception unit 107 per-

forms transmission/reception of packets with the VPN 4. Also a translation unit 106 performs address translation of a packet transmitted/received between the LAN and the VPN 4 based on the address translation information of FIG. 5C which an address management unit 104 holds. Additionally, the address management unit 104 performs address assignment processing in step S12 of FIG. 3, address determination processing in step S16, destination address communication processing in step S17, or the like. Furthermore, it performs the query to the DNS server in step S36.

[0023] An authentication management unit 103 performs authentication processing illustrated in step S11 of FIG. 3. Furthermore, the authentication management unit 103 queries the controller 2 as to whether communication via the VPN 4 with a query target communication apparatus is permitted for a communication apparatus that performed an IP address query by executing the processing of step S14 and step S15, or makes the determination by the information of FIG. 5C. A controller cooperation unit 101 performs processing for communication with the controller 2. A DNS cooperation unit 102 performs the processing for obtaining an IP address from the external DNS server in step S36 of FIG. 4.

[0024] Note, the present invention is not limited to the embodiment described above, and it is possible to make various modifications or changes without departing from the spirit and scope of the present invention. For example, in the explained embodiments, the LANs 31, 32 and 33 are assumed to be networks of different companies, but the present invention can be applied even if they belong to the same company. This is because even if it is the same company, there is an advantage that address adjustment, or the like, between locations becomes unnecessary. Accordingly, the following claims are attached to make public the scope of the present invention.

[0025] This application claims priority from Japanese Patent Application No. 2013-064872, filed March 26, 2013, which is hereby incorporated by reference herein in its entirety.

Claims

1. A transfer apparatus connected to a first network and a virtual private network and for transferring a packet between the first network and the virtual private network for communication between a communication apparatus of the first network and a communication apparatus of a second network via the virtual private network, the transfer apparatus comprising:

determination means for determining, when a request to communicate with a second communication apparatus of the second network or a query for an address of the second communication apparatus is received from a first communication apparatus of the first network, whether

communication between the first communication apparatus and the second communication apparatus via the virtual private network is permitted; and

address determination means for determining, when communication between the first communication apparatus and the second communication apparatus via the virtual private network is permitted, a destination address that the first communication apparatus uses when communicating with the second communication apparatus, and for notifying the first communication apparatus of the destination address.

2. The transfer apparatus according to claim 1, wherein the destination address that the address determination means determines is an address that does not overlap with an address of a communication apparatus that connects to the first network.
3. The transfer apparatus according to claim 1 or 2, wherein the determination means queries, when not holding information that communication between the first communication apparatus and the second communication apparatus via the virtual private network is permitted, a controller of the virtual private network as to whether communication between the first communication apparatus and the second communication apparatus via the virtual private network is permitted.
4. The transfer apparatus according to any one of claims 1 to 3, further comprising transmission means for translating, when a packet including the determined destination address is received from the first communication apparatus, the destination address of the packet and a transmission source address of the packet into predetermined addresses used in the virtual private network, and for transmitting to the virtual private network.
5. The transfer apparatus according to claim 4, wherein the transmission means performs the translation to the predetermined addresses used in the virtual private network in accordance with a combination of the destination address of the packet and the transmission source address of the packet.
6. The transfer apparatus according to claim 4 or 5, wherein the predetermined addresses used in the virtual private network are obtained from a controller of the virtual private network.
7. The transfer apparatus according to any one of claims 1 to 6, wherein the address determination means queries, when communication between the first communication apparatus and the second communication apparatus via the virtual private network

is not permitted, a sever on the Internet for the address of the second communication apparatus, and, when the address of the second communication apparatus can be obtained from the server on the Internet, notifies the first communication apparatus of the obtained address. 5

8. The transfer apparatus according to any one of claims 1 to 7, wherein the determination means manages, when communication between any one of a plurality of communication apparatuses of the first network and any one of a plurality of communication apparatuses of the second network via the virtual private network is permitted, the plurality of communication apparatuses of the first network and the plurality of communication apparatuses of the second network as a group. 10 15 20 25 30 35 40 45 50 55

FIG. 1

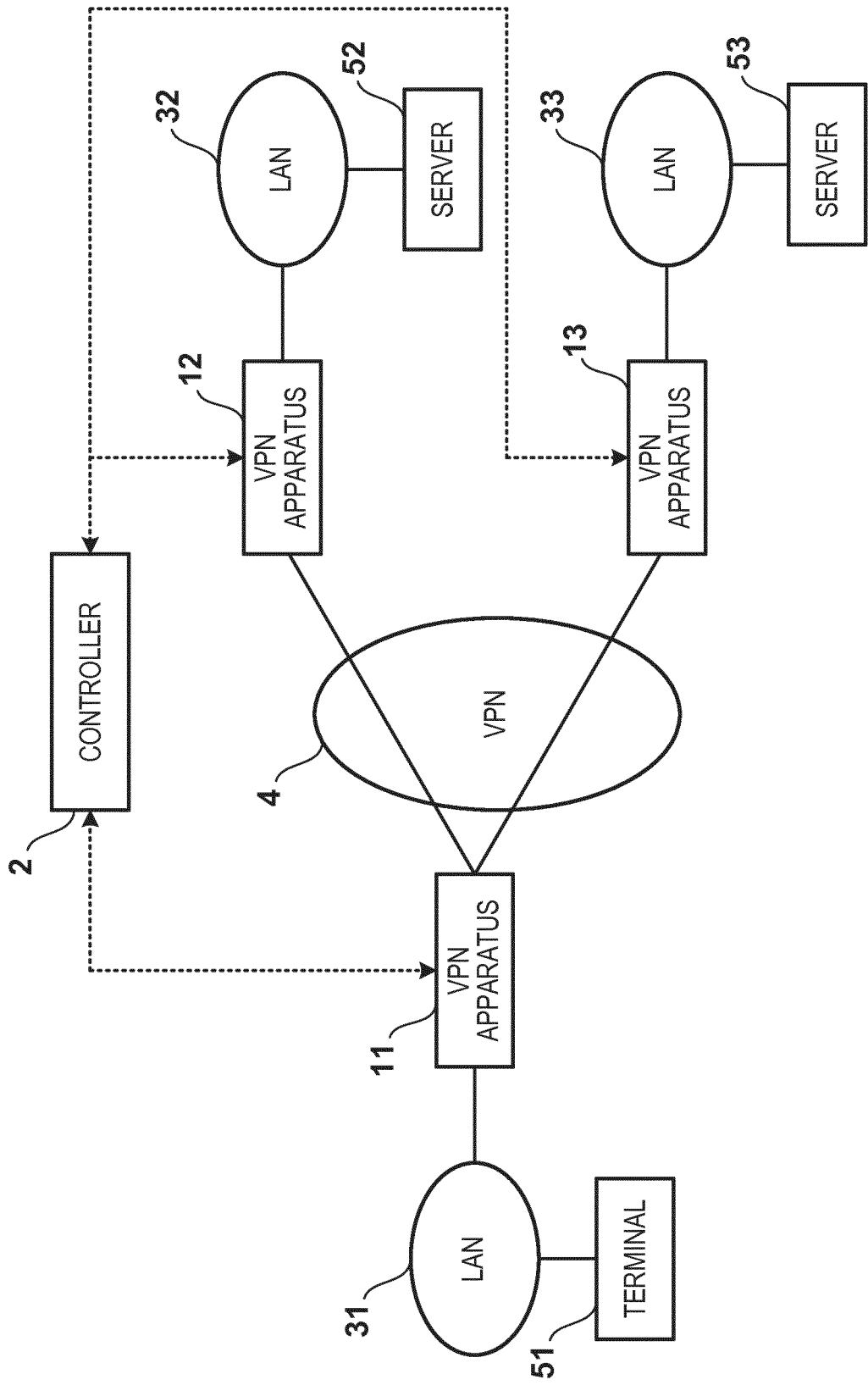


FIG. 2

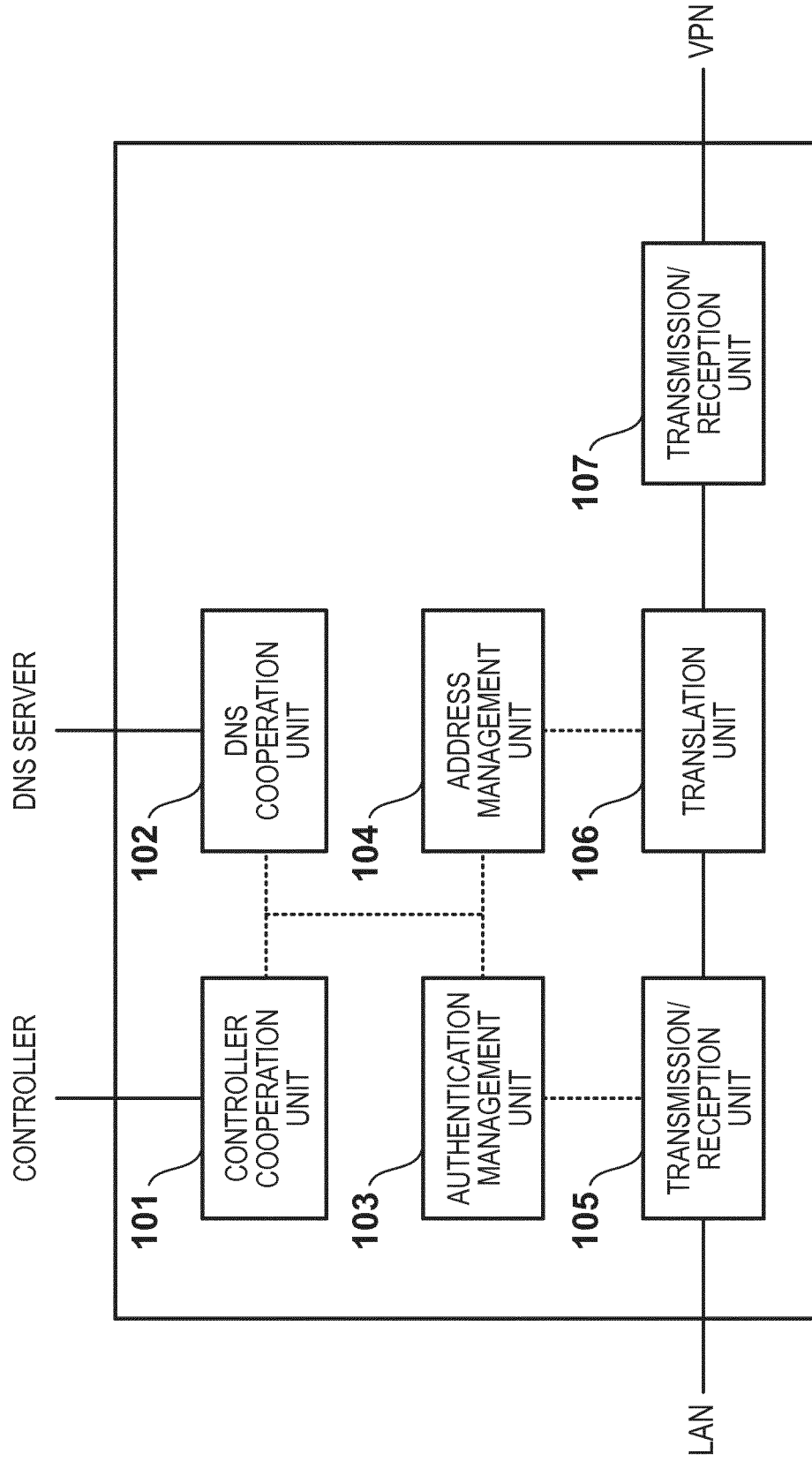


FIG. 3

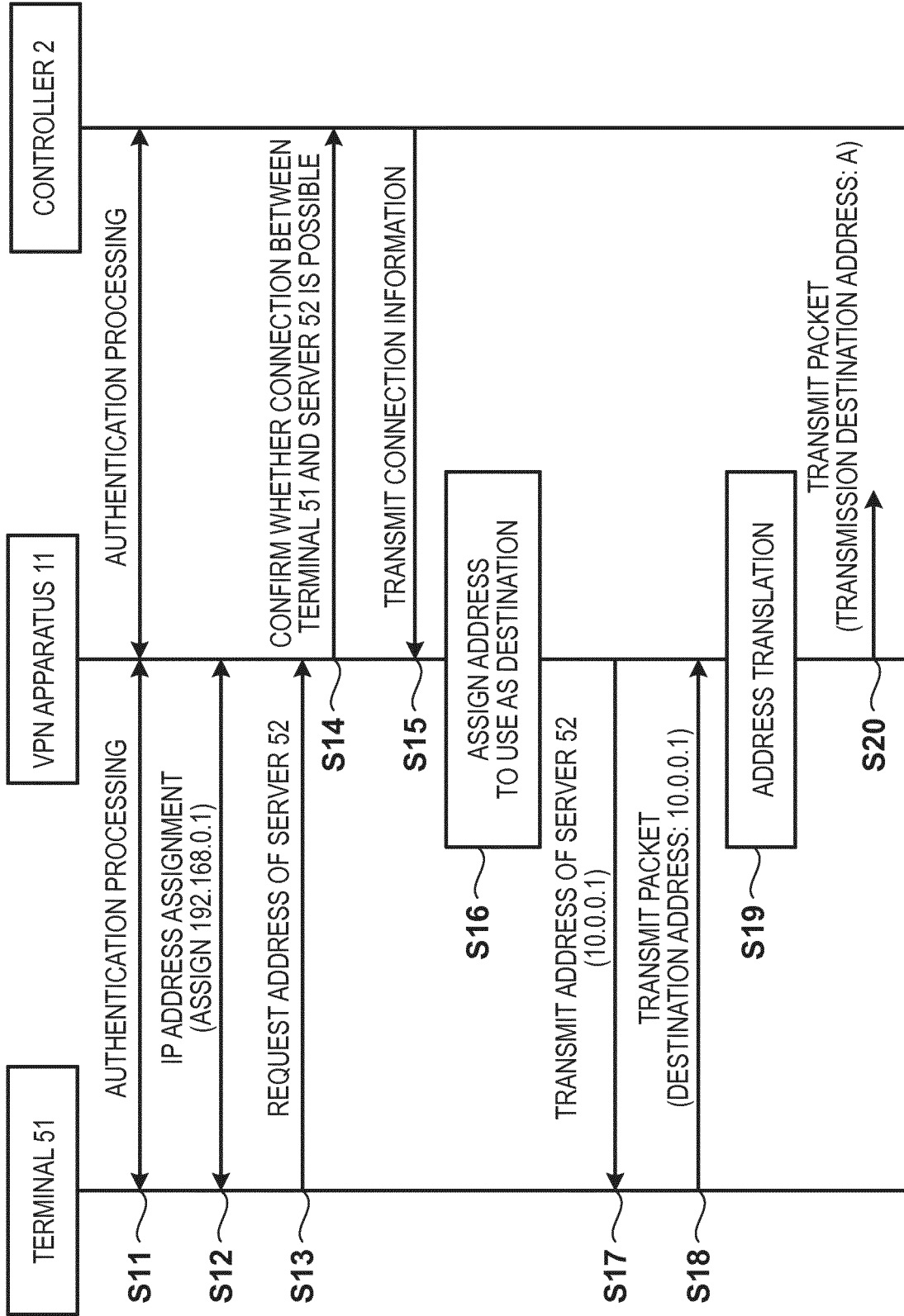


FIG. 4

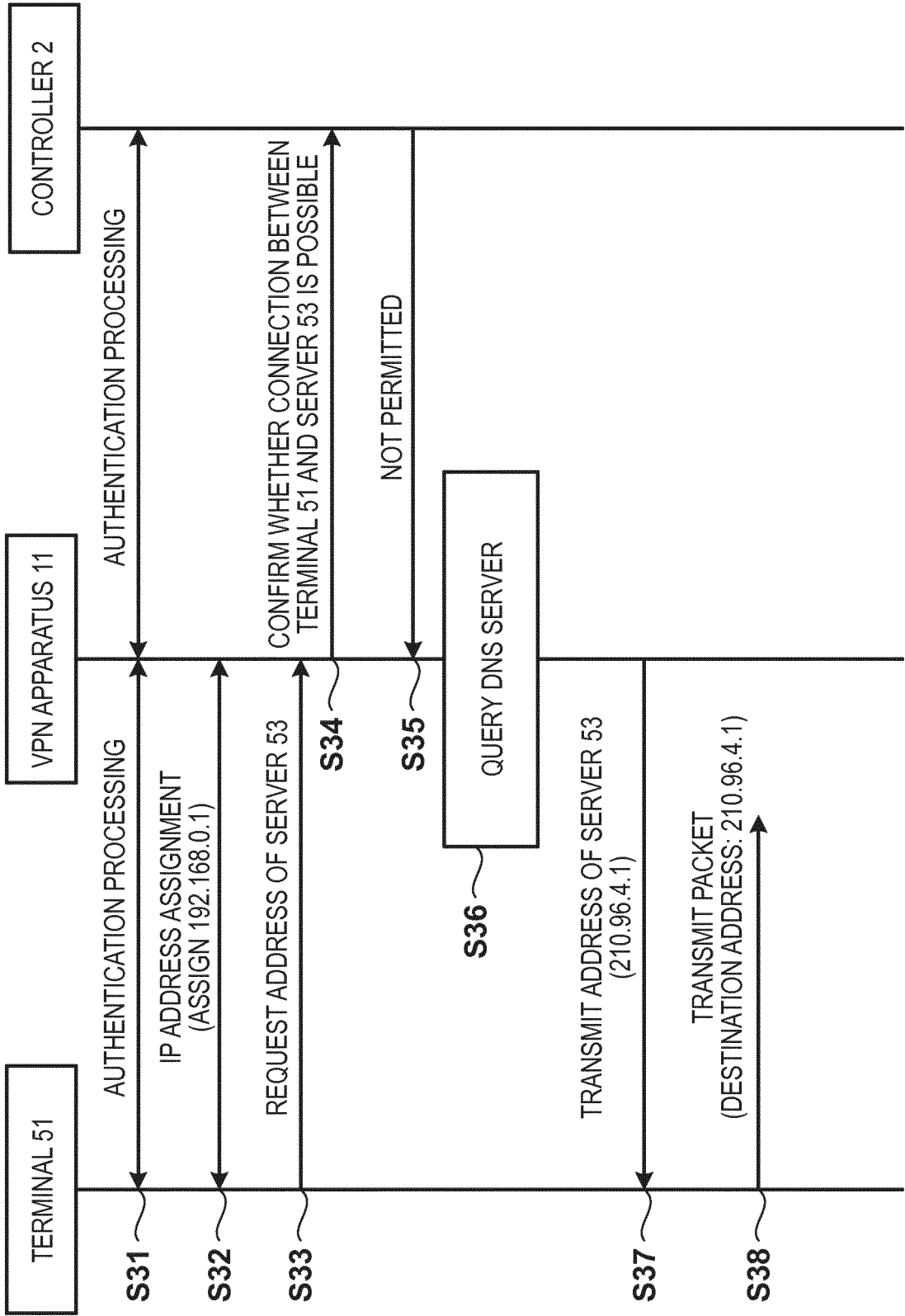


FIG. 5A

| | APPARATUS ID 1 | APPARATUS ID 2 | APPARATUS ID 1: VPN SIDE ADDRESS | APPARATUS ID 2: VPN SIDE ADDRESS |
|-----|----------------|----------------|----------------------------------|----------------------------------|
| #1 | TERMINAL 51 | SERVER 52 | X | A |
| #2 | TERMINAL 51 | SERVER xy | X | B |
| ... | ... | ... | ... | ... |

FIG. 5B

| GROUP ID | APPARATUS ID | VPN SIDE ADDRESS |
|----------|--------------|------------------|
| #1 | TERMINAL 51 | X |
| | SERVER 52 | A |
| | ... | ... |
| #2 | TERMINAL 51 | Y |
| | ... | ... |

FIG. 5C

| APPARATUS ID | IP ADDRESS | VPN SIDE ADDRESS |
|--------------|-------------|------------------|
| TERMINAL 51 | 192.168.0.1 | X |
| SERVER 52 | 10.0.0.1 | A |

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/001338

A. CLASSIFICATION OF SUBJECT MATTER

H04L12/46(2006.01)i, H04L12/70(2013.01)i, H04L12/749(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L12/46, H04L12/70, H04L12/749

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

| | | | |
|---------------------------|-----------|----------------------------|-----------|
| Jitsuyo Shinan Koho | 1922-1996 | Jitsuyo Shinan Toroku Koho | 1996-2014 |
| Kokai Jitsuyo Shinan Koho | 1971-2014 | Toroku Jitsuyo Shinan Koho | 1994-2014 |

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|---|-----------------------|
| Y A | JP 2012-80274 A (Brother Industries, Ltd.), 19 April 2012 (19.04.2012), paragraphs [0029] to [0056]; fig. 3 (Family: none) | 1-6, 8 7 |
| Y A | JP 2008-154066 A (Fujitsu Ltd.), 03 July 2008 (03.07.2008), paragraphs [0029] to [0030]; fig. 1, 2 & US 2008/0162516 A1 | 1-6, 8 7 |

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
26 March, 2014 (26.03.14)Date of mailing of the international search report
08 April, 2014 (08.04.14)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- JP 2005142702 A [0003]
- JP 2003101569 A [0003]
- JP 2013064872 A [0025]